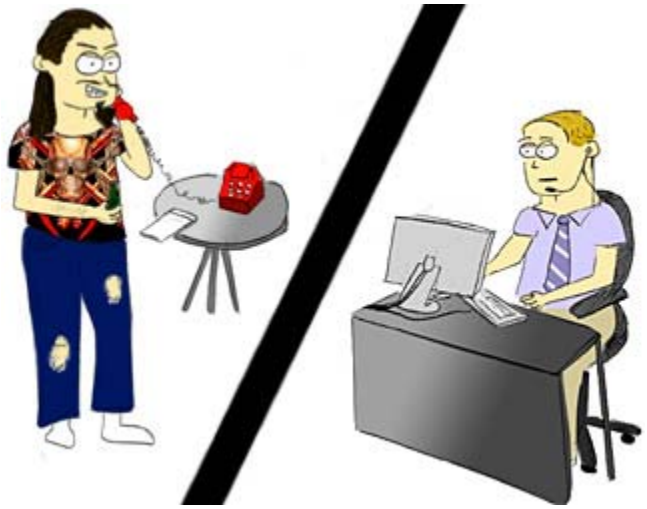
Security Quickie 8-28-02: Social Engineering

"Hello, this is Widgets, Inc. technical support."
"Hi, this is Matt Hague. I'm in a meeting with one of our customers, but I can't get to my share account to show our new database to them. Can you reset my password or somehow get me access to my account? This is really embarrassing, but I really need your help…"
"Uh, I'm not sure I can do that right now sir- "
"Listen, they have a flight in three hours, and this was the only chance for me to show them the new product. Something somewhere broke down and I can't get in to my system. I really need this to get done *now*. If I don't get this presented they could go with another company's product… can you get this done for me or not?!?"
"Well, I guess so. Just a minute and I'll get the information for you."
"(Sigh.) Thanks a lot! You're really going to save me. I really appreciate this. The account name is MHague."
"Ok, Matt, I'm getting the password now. It's JH5a2$$0."
"Thanks, you're a life saver. Bye."



Ever happen to you? The above is an example of a Social Engineering attack. Social Engineering is when an intruder attempts to gain information simply by using social interaction and manipulating an unsuspecting person into divulging information or gaining physical access to an area. In the above example an attacker, claiming to be the salesman Matt Hague, called Widget Inc.'s support center and gained confidential information via the phone. Social Engineering can also happen in other ways to: in person, by e-mail, over chat lines, via postal mail, or any other method that involves social interaction. Attackers can plead, beg, demand, threaten, cajole, praise, or do whatever is necessary to get the information they want.

Don't share confidential information with persons that don't need it or shouldn't have it. It is often our nature to be helpful to others, but this can be used against our organization and against us. Don't share passwords with unknown and unverified persons. Don't allow unknown people access to your work area without an escort. Be nice, friendly, and caring, but don't give unknown people the keys to the kingdom… um, State. The best defense against Social Engineering is to be aware that it does happen, and to know what is appropriate to share, when it can shared, and with whom it can be shared with. If you do suspect someone is attempting to use social engineering to gain access to the State's information systems, report it immediately to your supervisor.. If you notice suspicious behavior regarding physical access, for the Capitol Complex call Post 16 at 281-5608, or for other areas call your local Police Department or Sheriff's Office.

In information security, it is the human factor that is most crucial. Indeed, the security of the State's IT systems begins and ends with people, and more appropriately, with each of us. It's up to us to defend against Social Engineering, because it is 'us' who can allow or deny unauthorized access to the State's systems.